DOCKET FILE COPY ORIGINAL

DOCKET FILE COPY ORIGINAL

GARDNER, CARTON & DOUGLAS

1301 K STREET, N.W.

SUITE 900, EAST TOWER

WASHINGTON, D.C. 20005

(202) 408-7100

FACSIMILE: (202) 289-1504

CHICAGO, ILLINOIS

WRITER'S DIRECT DIAL NUMBER
GRIER C. RACLIN
(202) 408-7160

December 19, 1994

Federal Communications Commission
1919 M Street, N.W.
Room 222
Washington, D.C. 20554

Re: CC Docket 92-115 CC 93-116

Dear Sir or Madam:

Enclosed for filing on behalf of the Mobile and Personal Communications 800 Section of the Telecommunications Industry Association are an original and ten copies of a Motion for Stay, and a Petition for Clarification and Reconsideration in the above referenced docket.

All questions regarding these pleadings can be referred to the undersigned.

Sincerely,

Grier C. Raclin

Enclosures

cc: All Commissioners

DOCKET FILE COPY ORIGINAL

Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services	)	CC Docket No. 92-115
Amendment of Part 22 of the Commission's Rules to Delete Section 22.119 and Permit the Concurrent Use of Transmitters in Common Carrier and Non-common Carrier Service	)	CC Docket No. 94-46 RM 8367
Amendment of Part 22 of the Commission's Rules Pertaining to Power Limits for Paging Stations Operating in the 931 MHz Band in the Public Land Mobile Service	)	CC Docket No. 93-116

TO: THE COMMISSION

PETITION FOR CLARIFICATION AND RECONSIDERATION

THE MOBILE AND PERSONAL COMMUNICATIONS 800 SECTION OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: Grier C. Raclin, Esq.
Francis E. Fletcher, Esq.
Anne M. Stamper, Esq.
Gardner, Carton & Douglas
1301 K Street., N.W.
Suite 900, East Tower
Washington, D.C. 20005
Its Attorneys

Eric J. Schimmel; Vice President
James Caile; Chairman,
Mobile and Personal Communications 800 Section
Telecommunications Industry Association
2500 Wilson Blvd.
Suite 300
Arlington, Virginia 22201

Dated: December 19, 1994

TABLE OF CONTENTS

SUMMARY

The Mobile and Personal Communications 800 Section of the Telecommunications Industry Association ("TIA"), by this Petition, requests the Federal Communications Commission ("FCC" or "Commission") to reconsider certain provisions of Section 22.919 of the Commission's Rules as recently adopted in the *Report and Order* released in the docket on September 9, 1994. The Commission implemented these provisions, which require increased protection of Electronic Serial Numbers (ESNs), to combat the continuously increasing problem of cellular fraud. In part, the provisions require that ESN be "factory set and ... not ... alterable, transferable, removable or otherwise able to be manipulated." See 47 C.F.R. § 22.919(c) (effective January 1, 1995).

First, TIA requests the Commission to clarify that manufacturers' authorized representatives *may* transfer ESNs in connection with the repair and service upgrade of equipment that receives type-acceptance approval before January 1, 1995. Second, TIA requests the Commission to reconsider its decision to prohibit manufacturers' authorized representatives from altering the ESNs of equipment that receives type-acceptance *after* January 1, 1995. TIA asserts that the ESN "hardening" required by new Section 22.919 is an expensive and ineffective method of fighting cellular fraud. The Rule severely interferes with manufacturers' repair and service upgrade procedures, and prohibits manufacturers' authorized representatives from altering ESNs in the field will substantially increase the cost, and decrease the quality of service and equipment, to customers. Moreover, the implementation of the Rule may significantly and adversely affect the ability of TIA's members to export their products. These costs clearly outweigh the benefits provided by ESN hardening, because ESN hardening will never be

successful as long as ESNs or relied upon for billing verification and because the industry's authentication methodologies will be far more effective that the ESN hardening ordered by the Commission.

Finally, TIA believes that mandatory authentication procedures using the already defined framework of TIA TR45 is the proper answer to the fraud problem. Authentication is far superior to ESN hardening because it removes ESN data as a basis for fraud and provides a clear distinction on the air interface between authenticating and non-authenticating phones. Contrary to the Commission's concerns, authentication will not interfere with cellular operator's implementation of cellular "extension phone" service.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services	)	CC Docket No. 92-115
Amendment of Part 22 of the Commission's Rules to Delete Section 22.119 and Permit the Concurrent Use of Transmitters in Common Carrier and Non-common Carrier Service	)	CC Docket No. 94-46 RM 8367
Amendment of Part 22 of the Commission's Rules Pertaining to Power Limits for Paging Stations Operating in the 931 MHz Band in the Public Land Mobile Service	)	CC Docket No. 93-116

PETITION FOR CLARIFICATION AND RECONSIDERATION

The Mobile and Personal Communications 800 Section of the Telecommunications Industry Association ("TIA"), by its counsel, and pursuant to Section 405 of the Communications Act of 1934, as amended, and Section 1.106 of the Commission's Rules, hereby petitions the Federal Communications Commission ("FCC" or "Commission") for clarification and reconsideration of certain provisions of Section 22.919 of the Commission's Rules as adopted in the *Report and Order* released in this proceeding on September 9, 1994 (the "*Report and Order*").[1] Specifically, TIA hereby requests the Commission to:

---

[1] TIA is filing this Petition to solicit the Commission to make minor modifications to its Rules in an attempt to combat cellular fraud in the most cost-effective way possible. TIA did not participate in earlier stages of this proceeding because certain of its members and CTIA presented to the FCC the position that TIA would have advocated had it participated directly. As set forth herein, the Commission declined to adopt some of those

(a) clarify that new Rule 22.191 allows manufacturers' authorized field agents to transfer Electronic Serial Numbers (ESNs) in connection with the repair and upgrade of cellular subscriber units that receive FCC Type-Acceptance approval prior to January 1, 1995;

(b) reconsider its decision so as to allow manufacturers' authorized field agents to transfer ESNs in connection with the repair and upgrade of cellular subscriber equipment that receives Type-Acceptance approval after January 1, 1995; and

(c) reconsider its decision so as to require cellular subscriber equipment sold in the United States to comply with TIA-sanctioned authentication standards.

In support of this Petition, TIA states as follows:

I. BACKGROUND

A. The Telecommunications Industry Association

1. The Telecommunications Industry Association is the nation's largest organization of telecommunications equipment manufacturers. Its Mobile and Personal Communications 800 Section includes in its membership virtually all major cellular telephone system and mobile equipment manufacturers. The Association's 587 members provide products and services worldwide, and collectively have annual sales exceeding $20 Billion. TIA's members are directly impacted by the problem of cellular fraud and by any Commission proposed remedy to cellular fraud that affects the way members' products are manufactured, repaired or upgraded.

2. TIA has steadfastly supported the FCC's and industry efforts to fight and overcome cellular fraud, and will continue to do so in the future. The historical development of cellular anti-fraud designs and features implemented by TIA members manifests TIA's consistent and unwavering support of the FCC's, the Cellular Telephone Industry Association's (CTIA's), law enforcement agencies', and the public's efforts to overcome the fraudulent use of cellular

---

positions, which requires TIA to participate at this stage. See 47 C.F.R. § 1.106(b)(1). This Petition is timely filed under Sections 1.4 and 1.106 of the Rules.

telephones. It is important to note that this Petition is offered *to enhance* -- not to undercut -- such efforts. TIA firmly believes that the Rules resulting from a grant of this Petition will offer and provide to the public the most cost-effective weapons to use in the battle against cellular fraud.

B. Electronic Serial Numbers

3. An Electronic Serial Number ("ESN") is an identifying number that is uniquely assigned to each mobile, transportable, and portable cellular subscriber unit. At the time of "call setup," when the unit initiates a call or is polled for a call directed to it, the unit's ESN is transmitted without encoding to the relevant system's switch along with the unit's Mobile Identification (or telephone) Number ("MIN"). In present-day systems, if the calling or polled unit is a "roamer" in the system's service area, the ESN/MIN pair is transmitted via the inter-system network (that was established in conformance with TIA's Interim Standard ("IS")-41) to the unit's "home system." The local or distant home system compares the unit's transmitted ESN/MIN combination with information contained in its records to make sure the combination matches ESN/MIN pairing information for authorized users. If the MIN/ESN combination transmitted by the unit does not match with the system's data, the call may be blocked by the system operator.

4. Cellular telephone systems use ESNs to identify units for call-billing purposes. Even in the earliest days of cellular system design, it was recognized, therefore, that protecting ESNs from alteration by unauthorized individuals, or from unauthorized transfers to phones not owned by an authorized user, was important to assure accurate call billing. For this reason, the original cellular system design description, issued by AT&T Bell Laboratories' Advanced Mobile

Phone Service in October 1982, specified that ESNs should be "stored in a read only memory (ROM) suitably capsulated and mounted in a mobile unit." Id. at ¶ 1.7.2. Similarly, the FCC's original "Cellular System Mobile Station -- Land Station Compatibility Specification," OST Bulletin No. 53, July, 1983, specified that ESNs

> must be factory set and not readily alterable in the field. The circuitry that provides this serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative.

5. Unfortunately, as cellular system and subscriber unit design evolved, the opportunities for the fraudulent transfer and misuse of ESN/MIN combinations also increased. With each new technological development designed to combat cellular fraud came an offsetting development in the tools and technology available to fraudulent users. For example, when the simple electronic ESN passwords used in early system design proved inadequate, TIA members' designed and implemented ESN encryption, and later implemented the use of "flash memories" to store and process ESN information. When fraudulent users of cellular telephones attempted to masquerade as legitimate roaming users by transmitting random ESN/MIN pairs to local systems, TIA members designed and implemented changes to the inter-system call processing network, which was designed in conformance with TIA's Interim Standard ("IS")-41, to allow real-time inter-system verification of ESN/MIN pairs.

6. Perhaps the most illustrative of TIA members' efforts to fight cellular fraud is the recent adoption by TIA's Wireless Standards ("TR45") Committee, in association with CTIA representatives, of standards for the installation and use of cellular cryptographic authentication procedures and features. These standards were first proposed in 1989 in connection with the TDMA Dual Mode telephones because they offered a superior way to verify authorized

subscriber unit usage without the risks associated with the reliance on ESNs for this purpose. After three year's work, the standards were adopted and described in 1992 for TDMA dual mode phones in TIA's IS-54B TDMA Dual Mode system specification. TIA members then worked to expand the adoption of authentication standards for other equipment, and successfully did so to include inter-system signaling as described in IS-41 in 1992; CDMA dual mode phones as described in IS-95 in 1993; and AMPS and NAMPS analog telephones equipment as described in IS-91 in 1994. Even now, TIA is working to expand the adoption of authentication standards to include new TDMA single mode telephones as described in IS-136, and Personal Communications System ("PCS") equipment to be described in an upcoming Interim Standard. In all cases, the proposed authentication standards were subject to rigorous industry analysis, and laboratory and field testing, and are being implemented into current generation equipment. In all, TIA members have spend *many* years of labor and *many millions* of dollars designing, testing and deploying authentication technology as a replacement for the imperfect ESN-based anti-fraud verification system.

C. New Rule Section 22.919

7. In Comments filed in this proceeding, CTIA proposed that the FCC make TIA's authentication standards mandatory so as to require all cellular subscribed units that are sold in the United States and manufactured after a certain date to comply with the TIA and industry-backed authentication standards. CTIA Comments at 8. Rather than rely upon the industry's proposed authentication methodology to combat cellular fraud, however, the Commission instead adopted rules requiring the further protection -- or "hardening" -- of ESNs. The Commission rejected CTIA's proposal on the basis that implementation of the authentication procedures

"could have the unintended effect of precluding multiple cellular telephones (each with a unique ESN) from having the same telephone number." *Report and Order* at ¶59. In short, the FCC's decided to continue to address cellular fraud by attempting to make cellular phones incapable of accepting pirated ESNs, rather than removing the reliance on, and importance of, ESNs for billing purposes by adopting the authentication standards. New Rule Section 22.919 manifests this by deleting the term "readily alterable" from the old ESN protective language, replacing it with the requirement that ESNs "must be factory set and must not be alterable, transferable, removable or otherwise able to be manipulated." 47 C.F.R. Section 22.919.

8. Additionally, when adopting new Rule Section 22.919, the FCC rejected suggestions, made by CTIA and various equipment manufacturers, that the Commission modify its proposed rule to allow manufacturers' authorized service centers to transfer ESNs in the course their normal repair activities. *See, e.g.* CTIA Comments at 8, and Ericsson Corporation Comments at 2-5. These parties noted that such ESN transfers were crucial to manufacturers' repair and service upgrade procedures, without which subscriber units would have to be shipped to manufacturers' repair sites to remove or transfer ESN from equipment, at tremendously greater cost and inconvenience to subscribers. In rejecting these proposals, the Commission noted its fear that

> computer software to change ESNs, which is intended to be used only by authorized service personnel, might become available to unauthorized persons through privately operated computer 'bulletin boards'. We have no knowledge that it is now possible to prevent all unauthorized use of such software for fraudulent purposes. Accordingly, we decline to make the exception requested . . ..

Id. at ¶ 61.

II. THE COMMISSION SHOULD CLARIFY THAT MANUFACTURERS' AUTHORIZED FIELD AGENTS MAY TRANSFER ESNs IN CONNECTION WITH THE REPAIR AND UPGRADE OF PRE-1/1/95 EQUIPMENT

9. In its *Report and Order*, the Commission (as addressed in the text *infra*) declined to make an exception to the terms of new Section 22.919 to allow manufactures' authorized agents to undertake ESN transfers in connection with normal repair and upgrade activities. *Id.* at ¶61. At the same time, it agreed with certain commentators that "it would be impractical to apply the new rule to existing equipment," and therefore decided that "the ESN rule will apply only to cellular equipment for which initial type-acceptance is sought after the date that our rules become effective [January 1, 1995]." *Report and Order* at ¶62. The natural conclusion of these two decisions is that manufacturers' field agents *may* undertake ESN transfers and changes in connection with repair and upgrade activities associated with cellular equipment for which initial type-acceptance was sought *before* January 1, 1995, even if such repair activity takes place after January 1, 1995. Unfortunately, this point was left somewhat unclear in the *Report and Order* and TIA therefore requests that it be clarified at this time.[2] Similarly, the Commission's statement that a consumer's use of a subscriber unit with any altered ESN would be unlawful, *Report and Order* at ¶62, should be clarified to disallow only the use of equipment with ESNs that have been altered by other than manufacturer's authorized agents outside of normal repair and service upgrade activities.

---

[2] It is important to note that TIA is *not* seeking reconsideration of the Rule insofar as it prohibits ESN transfers that are not authorized by users and system operators, regardless of the relevant equipment date of type-acceptance approval.

III. THE COMMISSION SHOULD ALLOW MANUFACTURERS' AUTHORIZED FIELD AGENTS TO TRANSFER ESNs IN CONNECTION WITH THE SERVICE AND SERVICE UPGRADE OF POST 1/1/95 EQUIPMENT

10. The FCC should reconsider its decision to disallow manufacturers' authorized representatives from transferring or modifying ESNs in the course of their normal repair and service upgrade activities of equipment that receives type acceptance approval *after* January 1, 1995.[3] Implementation of the Commission's Rules as presently drafted will significantly and adversely affect the ability of TIA's members to repair and upgrade their subscriber units, thus greatly increasing the cost, and decreasing the quality, of service and equipment to consumers.

11. As outlined in Ericsson's initial comments filed in this proceeding, procedures presently utilized by virtually every cellular telephone manufacturer call for authorized repair agents to transfer ESNs from defective or old equipment to new equipment if they are incapable of repairing a subscriber unit quickly. This allows customers to enjoy ongoing service without the inconvenience and delays that would result from the FCC-mandated return of the units to the manufacturers' sites. Additionally, while ESN rarely cause or contribute to a unit's failure, manufacturers normally use the opportunity of repairing a unit to upgrade its software -- which normally includes the exchange of an ESN -- to include the latest features. Adoption of the FCC's Rule as written would (1) prohibit manufacturers from making these ESN transfers in the field even with the authorization of the subscriber; (2) require subscribers to reestablish service utilizing new ESNs while their defective units remain at the manufacturing plant for repair; (3) require manufacturers to incur (and pass on to consumers) the costs of returning defective units

---

[3] While the Commission implicitly decided that manufacturers *may* undertake ESN transfers directly (versus indirectly through their agents), §22.919 arguably would bar even these transfers by requiring that ESNs "must not be alterable, transferable, removable or otherwise able to be manipulated" by *any* party. TIA therefore requests the Commission to clearly state that ESN *may* be subject to transfers, etc., by manufacturers directly.

back to manufacturing sites to evaluate whether they should be repaired or discarded; (4) prohibit carriers from utilizing ESNs incorporated into defective units pending such evaluation and repair; and (5) prohibit service upgrades normally undertaken in connection with repair activities. In sum, adoption of the new Rule would tremendously disrupt currently established cellular telephone repair and upgrade practices.

12. The cost to manufacturers -- and thus to consumers -- resulting from implementation of the Commission's new ESN protective Rules will be substantial. Not only will substantial costs, possibly approaching $30 million, have to be incurred by the manufacturing community to design ESN-hardening software and hardware, but it would cost an additional $1.50 - $3.00 per-unit (or approximately *$100 million additional dollars*, given past growth patterns) to install such features into cellular subscriber units over the next year or two. Additionally, the cost for servicing defective units and upgrading the software of all units will rise substantially to account for the shipment of units back to manufacturing sites to transfer ESN as required or appropriate for repair and service upgrade activities. These shipment costs alone can approach $3.00 - $5.00 per unit, or *many millions* of dollars when the average number of repaired or upgraded units are considered. The sum of these costs either will have to be paid directly (in the case of units needing repair after the warranty period) or indirectly (in the case of repairs required during the warranty period) by consumers without (*see* text *infra)* any offsetting benefit. Indeed, to defer incurring these costs without any offsetting benefits, it is likely that manufacturers will delay the introduction of models requiring new Type-Acceptance Approvals, thus denying the public the advantages of technological advances.

13. Normally, given the increased costs required to implement the Commission's new Rule, it is likely that customers and manufacturers will simply discard defective units and units seeking service upgrades rather than incur the costs associated with shipping the units back to the manufacturers' sites to replace the associated ESNs. Indeed, some state warranty laws might *require* manufacturers to do this by requiring that all repair and upgrade of cellular units take place locally for a period of time after unit purchase. Because the FCC's new Rule Section 22.919 would effectively prohibit local repair activity that involves ESN transfers, service centers may have no choice but to discard units and ESNs in connection with local servicing. This discarding of telephone equipment, and its associated ESNs, would be tremendously wasteful and again would dramatically increase the cost of equipment and service to consumers.

14. Customer inconvenience, and the resulting loss of the consumers' goodwill towards the industry and their respective carriers, is a dramatic non-financial industry cost that would result from implementation of the Commission's new rules. This is especially true after telephone warranties expire, and consumers are forced directly to pay the entire cost of shipping the unit back to manufacturers' sites. If the consumer would decide not to bear such costs, he or she would be forced to either purchase an entire new telephone, or terminate service. Neither option should prove attractive to the industry or the Commission.

15. The Commission also was incorrect in surmising that ESN-altering software could not be protected while in the hands of manufacturers' authorized repair agents. Ericsson's Reply Comments outline one option utilized by many manufacturers to protect ESN-altering software. In addition, it is likely that this software could be protected using either symmetric or asymmetric key cryptography similar to that which underlies the authentication protections being installed in

new generation telephones (*see* text *infra*). Under this procedure, the repair agent could obtain access to ESN software only by inputting a digitized "signature" that would be safe from unauthorized access at the manufacturer's own repair location *and* in the field equally.

16. Indeed, while no protection of ESN-modifying software would be totally fool-proof, there is no reason to believe that software located at manufacturers' agents service locations will be any less secure than software located at the manufacturers' own manufacturing sites. TIA members will, of course, undertake all reasonable efforts to protect ESN-altering technology that is located at its agents sites, and the FCC might condition the right of manufactures' agents to modify ESNs upon their use of this protective processes. *See* Attachment A. It appears from historical investigations, in fact, that the first use of pirated ESN modifying software arose not in United States at all (and certainly not from a break-in at a repair agent's location), but in connection with *ETACS* equipment that was manufactured and sold in *England* and *Greece*. Quite simply, so long as the Commission continues to rely upon ESNs to verify the identity of subscriber equipment for call billing purposes, and the FCC's own compatibility standards (as set forth in OST-53) require ESNs to be broadcast without encoding, there is virtually no protection that the FCC can implement to totally safeguard ESN modifying technology. The better step is as proposed by CTIA -- to rely upon new authentication methodologies rather than ESNs for this purpose.

IV. THE COMMISSION SHOULD MANDATE CELLULAR SUBSCRIBER UNITS' COMPLIANCE WITH INDUSTRY AUTHENTICATION STANDARDS

17. Given the defects of ESN-based billing verification technology, the Commission should also reconsider its decision not to make TIA's authentication standards mandatory for all telephones receiving Type Acceptance approval after a reasonable date, which TIA proposes to be September 1995. The authentication methodology is a far superior, more efficient, and less costly method of combating cellular fraud than the ESN "hardening" adopted by the FCC. The benefits associated with utilizing authentication to prevent cellular fraud clearly outweigh any costs associated with eliminating the Commission's ESN hardening rule. Moreover, contrary to the FCC's concerns, adopting of the authentication requirements will *not* prohibit or even interfere with the provision of cellular extension phone service. While the basis of the Commission's concern is not clear in the *Report and Order*, TIA's service standards as set forth in IS-53 address the need for differentiating among telephones with the same MIN in a variety of ways, including the use of "cellular hunt groups" that prioritize the extensions utilizing the same MIN for call delivery purposes. Requiring cellular subscriber equipment to satisfy industry-accepted standards will assure compliance with the Commission's overall compatibility requirements.

18. As indicated above, notwithstanding the best efforts of TIA , CTIA, law enforcement agencies, and the general public, ESNs can never be fully protected so long as they are broadcast "in the clear" during call set-up processes as required by OST-53. The design of cellular systems complying with OST-53 (*i.*e., all of them) calls for ESN-based verification to occur within the system switch, which requires ESNs to be broadcast by subscriber units, without

encoding, to the relevant systems for verification. They simply cannot be totally protected from creative interception and decoding techniques, or misuse by sophisticated criminals. Even if the Commission were to require the transmission of encoded ESNs using the polynomial multiplication/division, cyclic coding, or bit spreading technologies specified in the Rule, these advanced technologies eventually will be overcome by dedicated, sophisticated criminals utilizing equally up-to-date technologies and equipment. In short, the fundamental flaw in the Commission's new Rule Section 22.919 is its continued reliance upon ESN-based caller verification in the first place. Even if, contrary to the lessons of the past, new hardening techniques can be protected from invasion by equally "hardened" criminals, this reliance on ESNs utterly ignores the fact that ESNs can still be "stolen" over-the-air, and inserted into the *20+ million* subscriber units that are active today, and the many millions more that may be manufactured offshore in the future that will *not* incorporate hardened ESNs.[4]

19. TIA's authentication is a superior method to protect against cellular fraud because it does not rely upon the open transmission of ESN or similar information to verify callers for call billing purposes. Rather, authentication methodologies render ESNs obsolete for billing purposes by separating the identification of mobile equipment required by the manufacturers for repair, service upgrade and other similar purposes, from the identification of mobile equipment required by the carriers for call billing purposes. Whereas ESN still would be utilized to serve the former purpose, the authentication methodology would be used for call billing verification.

[4] Indeed, even assuming the ESN hardening requirements adopted by the Commission, new generation phones might be subject to "Class C" counterfeiting in which the ESN protections are irrelevant because the phones' *entire code set* -- including the encoded ESN -- is removed and replaced with other information, including fraudulently obtained ESNs.

20. With authentication methodology, the identity of a subscriber unit for billing purposes is obtained from a cryptographic variable, called an "Authentication-" or "A-Key", that is never broadcast over the air, but rather resides, protected, in the cellular subscriber unit. The A-Key is alterable by the subscriber, and is shared with the System by means other than over-the-air transmissions. At the time of call set up, a cryptographic "Challenge" is broadcast by the system to the mobile unit. The Challenge need not be protected from interception because it is worthless without the A-Keys associated with polled subscriber units. When it receives a Challenge, the subscriber unit computes a "Response" that is mathematically based on its A-key, the Challenge, and other data that is shared with the system (such as portions of its ESN, its MIN and similar information) according to an algorithm that also is shared with the system.[5] The System is, therefore, equally capable of calculating the mobile station's expected response to its challenge. If the mobile station's calculated Response equals the system's expectation, the authentication process is satisfied. If not, the mobile station can be denied service.

21. The authentication methodology is far more secure than the ESN-based verification methodology because the information that is broadcast -- the Challenge and the Response -- is useless without the A-Key that is integrated into the subscriber's actual unit and never broadcast. The algorithm used in the process is "one-way path," which means that it is virtually impossible to derive its input information (such as the A-Key) from its calculated conclusion. It is practically impossible to derive the A-Key from the Response, even if the Challenge, and other information used in the algorithm is known. While it may be theoretically possible to "reverse engineer" the A-Key from this information, it is estimated that there is only

[5] This method is based on an algorithm called CAVE which has been determined by the Office of Defense Trade Controls to be a Category 13, Subsection B, U.S. Munitions List Cryptographic Technology.

a 1 in 2^{128} chance of correctly guessing a private A-Key consistent with available information. The Commission must compare that success rate to the 100% chance of determining an ESN once it is intercepted.[6]

22. Importantly, it is likely that authentication will be implemented in the marketplace *long before* the FCC's new ESN regulations would become applicable. It is estimated that it will require approximately 9-12 months to design, manufacture and deploy cellular telephone units incorporating the ESN hardening protections outlined by the Commission. Authentication methodologies, on the other hand, have already been through the design and acceptance phase; have been approved by the relevant TIA and CTIA representatives and technical committees; have been reviewed by relevant export authorities; and are now being installed, and are appearing, in subscriber units being sold to the public. In all likelihood, these authentication features will be fully deployed in new-generation equipment within a 6-9 month time-frame. Given these circumstances, the adoption of ESN hardening protections outlined by the FCC are totally unnecessary and inferior to the authentication methodologies already being adopted by the industry.

23. Finally, implementation of the Commission's Rule may significantly and adversely affect the ability of TIA's members to export their products. Present export restrictions prohibit the transfer or export of certain high technology processes, procedures and equipment without proper authorization from the appropriate U.S. Government agency. The need to obtain these authorizations could significantly delay shipments of TIA products. In some instances, the

---

[6] Even the chance of loss resulting from this one-in-a-million event can be reduced by the concurrent use of the many fraud-fighting software on the market, as described in "Fending Off Fraud" appearing in the September, 1994 edition of *Cellular Business* at p. 32.

cognizant U.S. Government agency could deny authorization based upon the level and type of encryption involved. Incorporation of the technology required to adequately harden ESNs may therefore well run afoul of export restrictions applicable to domestic cellular telephone equipment. Unlike the authentication methodology, which requires sophisticated software to be inserted into relatively unsophisticated microprocessors in subscribers units, ESN hardening methodologies likely to be used by manufacturers will require the insertion of sophisticated encryption hardware into subscriber units. The authentication software can be deleted from subscriber units intended for export far more easily and cheaply than the encryption hardware required for ESN hardening. Additionally, virtually all of the issues to be confronted with regard to the export of units incorporating authentication features have already been addressed by TIA members working with the relevant government agencies, whereas these efforts would have to be begin anew if the ESN hardening features are required by the Commission. In short, requiring ESN hardening will greatly disrupt and increase the cost of manufacturing cellular subscriber units for export because separate units would have to be manufactured for domestic and foreign systems. Moreover, the units that would be exported into foreign markets without ESN hardening features constitute a supply of units that might return to the United States in a "gray market," ready for fraudulent use, thus further undercutting the likelihood that the FCC's ESN hardening efforts would be successful.

V. CONCLUSION

24. For the foregoing reasons, TIA respectfully requests the Commission to clarify and reconsider certain provisions of Rule 22.919 as adopted in the *Report and Order* in this proceeding. The Commission should clarify that the Rule's ESN transfer prohibition does not

apply to manufacturers' authorized representatives in connection with the repair and service upgrade of equipment that receives type-acceptance before January 1, 1995. The Commission should reconsider parties' suggestion that it modify its proposed rule to allow manufacturers' authorized agents to transfer ESNs in the course of their normal repair activities. Implementation of ESN hardening is prohibitively expensive and will not accomplish the Commission's goal of combating cellular fraud.

Given the fact that authentication is the superior method for preventing cellular fraud, the Commission should reconsider its decision not to mandate cellular subscriber units' compliance with industry authentication standards. Authentication will not prevent the implementation of cellular extension service.

Respectfully submitted,

THE MOBILE AND PERSONAL COMMUNICATIONS 800 SECTION OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: _____

Grier C. Raclin, Esq.
Francis E. Fletcher, Esq.
Anne M. Stamper, Esq.
Gardner, Carton & Douglas
1301 K Street., N.W.
Suite 900, East Tower
Washington, D.C. 20005

Its Attorneys

Eric J. Schimmel; Vice President
James Caile; Chairman,
Mobile and Personal Communications 800 Section
Telecommunications Industry Association
2500 Wilson Blvd.

ATTACHMENT A

PROPOSED RULE SECTION 22.919

The Electronic Serial Number (ESN) is a 32 bit binary number that uniquely identifies a cellular mobile transmitter to any cellular system.

(a) Each mobile transmitter in service must have a unique ESN.

(b) The ESN host component must be permanently attached to a main circuit board of the mobile transmitter and the integrity of the unit's operating software must not be alterable, *except by authorized manufacturer service centers or representatives for the purpose of legitimate service repair or upgrade*. *Before authorized manufacturers service centers or representatives may alter or transfer ESNs, they must implement steps to protect the equipment and software they are using for such purposes from unauthorized use*. The ESN must be isolated from fraudulent contact and tampering. If the ESN host component does not contain other information, that component must not be removable, and its electrical connections must not be accessible. If the ESN host component contains other information, the ESN must be encoded using one or more of the following techniques:

(1) Multiplication or division by a polynomial;

(2) Cyclic coding;

(3) The spreading of ESN bits over various non-sequential memory locations.

(c) Cellular mobile equipment must be designed such that any attempt, *except by authorized manufacturer service centers or representatives for the purpose of legitimate service repair or upgrade*, to remove, tamper with, or change the ESN chip, its logic system, or firmware originally programmed by the manufacturer will render the mobile transmitter inoperative.

(d) Cellular mobile equipment receiving Type Acceptance approval after September 30, 1995, must comply with industry standards for authentication, as described in applicable Interim Standards issued by the Telecommunications Industry Association.

CERTIFICATE OF SERVICE

I, Christine Peyton, a secretary in the law firm of Gardner, Carton & Douglas, certify that I have this 19th day of December, 1994, caused to be sent by first-class, U.S. mail, postage prepaid, a copy of the foregoing PETITION FOR CLARIFICATION AND RECONSIDERATION AND MOTION TO STAY to the following:

Chairman Reed Hundt
Stop Code 0101
Federal Communications Commission
1919 M Street, N.W., Room 814
Washington, D.C. 20554

Commissioner Andrew C. Barrett
Stop Code 0103
Federal Communications Commission
1919 M Street, N.W., Room 826
Washington, D.C. 20554

Commissioner Rachelle Chong
Stop Code 0105
Federal Communications Commission
1919 M Street, N.W., Room 844
Washington, D.C. 20554

Commissioner James H. Quello
Stop Code 0106
Federal Communications Commission
1919 M Street, N.W., Room 802
Washington, D.C. 20554

Commissioner Susan Ness
Stop Code 0104
Federal Communications Commission
1919 M Street, N.W., Room 832
Washington, D.C. 20554

John Cimko, Chief
Mobile Services Division
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W., Room 644
Washington, DC. 20554

A. Richard Metzger, Chief
Common Carrier Bureau
Federal Communications Commission
2025 M Street, N.W., Room 500
Washington, D.C. 20554

Regina Keeney, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.
Room 5002
Washington, D.C. 20554

Gerald P. Vaughan
Deputy Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.
Room 5002
Washington, D.C. 20554

Stephen Markendorff
Commercial Radio Division
Wireless Telecommunications Bureau
Federal Communications Commission
1919 M Street, N.W.
Room 644
Washington, D.C. 20554

Laurence D. Atlas
Associate Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.
Room 5002
Washington, D.C. 20554

Daniel Phython
Sr. Legal Assistant to Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.
Room 5002
Washington, D.C. 20554

Richard M. Smith, Chief,
Office of Engineering and Technology
Federal Communications Commission
2025 M Street, N.W.
Room 7002
Washington, D.C. 20554

Bruce A. Franca, Deputy Chief
Office of Engineering and Technology
Federal Communications Commission
2025 M Street, N.W.
Room 7002
Washington, D.C. 20554

Julius Knapp, Chief
Authoriation and Evaluation Division
Office of Engineering & Technology
7435 Oakland Mills Road
Columbia, MD 21046

Richard Engelman
Chief, Technical Standards Branch
Office of Engineering and Technology
Federal Communications Commission
2025 M Street, N.W.
Room 7002
Washington, D.C. 20554

John Cimko, Jr.
Chief, Policy Division
Wireless Telecommunications Bureau
Federal Communications Commission
1919 M Street, N.W.
Room 644
Washington, D.C. 20554

Lawrence M. Miller
Schwartz, Woods & Miller
1350 Connecticut Ave., N.W.
Suite 300
Washington, D.C. 20036

Jil Abeshouse Stern
Shaw, Pittman, Potts
&N Trowbridge
2300 N Street, N.W.
Washington, D.C. 20037

David E. Weisman
Meyer, Faller, Weisman
and Rosenberg, PC.
4400 Jenifer Street, N.W.
Suite 380
Washington, D.C. 20015

R. Michael Senkowski
Jeffrey S. Linder
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Ellen S. Mandell
Louis Cybulski
Pepper & Corazzini
200 Montgomery Building
1776 K Street, N.W.
Washington, D.C. 20006

Thomas A. Stroup
Mark Golden
Telocator, The Personal
Communications Industry Association
Suite 1100
1019 19th Street, N.W.
Washington, D.C. 20036

Jeffrey L. Sheldon
Sean A. Stokes
Utilities Telecommunications Council
Suite 1140
1140 Connecticut Ave., N.W.
Washington, D.C. 20036